This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号
特開2000－188616
（P2000－188616A）
(43)公開日　平成12年７月４日(2000.7.4)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｅ	５Ｋ０３０
Ｈ０４Ｌ　9/16		Ｈ０４Ｌ　9/00	６４３	９Ａ００１

審査請求　未請求　請求項の数５　ＯＬ　（全８頁）

(21)出願番号　特願平10－362917

(22)出願日　平成10年12月21日(1998.12.21)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(71)出願人　000187725
松下通信工業株式会社
神奈川県横浜市港北区網島東４丁目３番１号

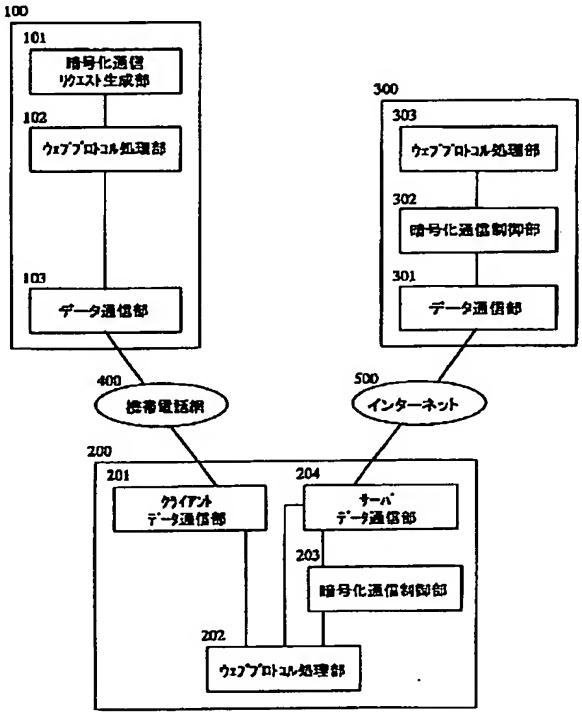
(71)出願人　392026693
エヌ・ティ・ティ移動通信網株式会社
東京都港区虎ノ門二丁目10番１号

(74)代理人　100099254
弁理士　役　昌明　（外３名）

最終頁に続く

(54)【発明の名称】　通信システム及び通信方法

(57)【要約】
【課題】　携帯電話網のような安全性が確保された通信網を経由してインターネットに接続し、電子商取引やバンキングサービスを実施する端末の負担を軽減できる通信システムを提供する。
【解決手段】　クライアント装置100の暗号化通信要求生成部101が、ゲートウェイサーバ装置200に対して通信経路での安全要求を送出し、これを受けてゲートウェイサーバ装置の暗号化通信制御部203が、コンテンツサーバ装置300との間で暗号化通信の設定を行ない、コンテンツサーバ装置が、クライアント装置に送信するデータを暗号化してゲートウェイサーバ装置に送信し、ゲートウェイサーバ装置の暗号化通信制御部が、このデータを復号化してクライアント装置に送信する。クライアント装置には暗号化・復号化の処理系が不要であり、負担が軽減される。



【特許請求の範囲】

【請求項１】　コンテンツデータを管理するコンテンツサーバ装置と前記コンテンツサーバ装置とは異なる通信網上に存在するクライアント装置とが、異なる通信網間を中継するゲートウェイサーバ装置を介して行なう通信方法において、　前記クライアント装置及びゲートウェイサーバ装置間の通信の安全性が確保されている場合に、前記クライアント装置及びゲートウェイサーバ装置間の通信網ではデータの暗号化は行なわず、セキュリティが確保されていない前記ゲートウェイサーバ装置及びコンテンツサーバ装置間の通信網による通信でのみデータの暗号化を行なうことを特徴とする通信方法。

【請求項２】　前記クライアント装置が、前記ゲートウェイサーバ装置に対して、通信経路での安全要求を送出し、これを受けて前記ゲートウェイサーバ装置が前記コンテンツサーバ装置との間で暗号化通信の設定を行ない、前記コンテンツサーバ装置が、前記クライアント装置に送信するデータを暗号化して前記ゲートウェイサーバ装置に送信し、前記ゲートウェイサーバ装置が、前記データを復号化して前記クライアント装置に送信することを特徴とする請求項１に記載の通信方法。

【請求項３】　前記クライアント装置が、前記ゲートウェイサーバ装置に対して、データの送信と併せて通信経路での安全要求を送出し、これを受けて前記ゲートウェイサーバ装置が前記コンテンツサーバ装置との間で暗号化通信の設定を行ない、前記データを暗号化して前記コンテンツサーバ装置に送信することを特徴とする請求項１に記載の通信方法。

【請求項４】　コンテンツデータを管理するコンテンツサーバ装置と前記コンテンツサーバ装置とは異なる通信網上に存在するクライアント装置とが、異なる通信網間を中継するゲートウェイサーバ装置を介して通信を行なう通信システムにおいて、

クライアント装置とゲートウェイサーバ装置との間が安全性が確保された通信網で接続され、

前記クライアント装置が、前記ゲートウェイサーバ装置との間でデータの送受信を行なうデータ通信手段と、前記データ通信手段を通じて前記クライアント装置及びコンテンツサーバ装置間の通信の安全要求を送出する暗号化通信要求手段とを備え、

前記ゲートウェイサーバ装置が、前記クライアント装置との間でデータの送受信を行なうクライアントデータ通信手段と、前記コンテンツサーバ装置との間でデータの送受信を行なうサーバデータ通信手段と、前記クライアント装置からの安全要求に従い前記サーバデータ通信手段を通じて前記コンテンツサーバ装置との暗号化通信の設定処理を行ない、前記サーバデータ通信手段から受信した暗号化されたデータの復号化と前記サーバデータ通信手段に出力するデータの暗号化とを行なう暗号化通信制御手段とを備えることを特徴とする通信システム。

【請求項５】　前記クライアント装置が、前記データ通信手段を通じて前記ゲートウェイサーバ装置との間でワールド・ワイド・ウェブのデータを送受信するためのウェブプロトコル処理手段を具備し、前記ゲートウェイサーバ装置が、前記クライアントデータ通信手段及び前記サーバデータ通信手段を通じてワールド・ワイド・ウェブのデータを送受信するためのウェブプロトコル処理手段を具備することを特徴とする請求項４に記載の通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クライアントとサーバが異なる通信網上に存在し、異なる通信網間を中継するゲートウェイサーバを介して通信を行なう通信システムと、その通信方法に関し、特に、暗号化通信を行なう場合のクライアント装置の負担を軽減するものである。

【０００２】

【従来の技術】近年、ワールド・ワイド・ウェブ（以下、ウェブ）の登場により、インターネット上で様々なサービスが提供されている。中でも、電子商取引やインターネットバンキングサービスは、今後さらに拡大することが予想されている。

【０００３】これらのサービスでは、セキュリティの確保が絶対条件であるが、現在のインターネットでは、データの盗み見が比較的容易であり、特にウェブでは、通常、データを暗号化せずにテキストとして送受信するため、セキュリティが十分確保されているとは言えない。

【０００４】現在、各種の公開鍵、共通鍵暗号や、ハッシュ関数によるデータのダイジェストを利用し、インターネット上のセキュリティを確保することが行なわれている。特に、ウェブにおけるクライアントとサーバ間でセキュアな通信を行なうためのプロトコルとして、ＳＳＬ（Secure Sockets Layer）が広く利用されている。

【０００５】例えば、特開平１０－１３５９４２号公報の「通信システム、メッセージ処理方法及びコンピュータ・システム」では、公開鍵暗号を用いたメッセージ処理通信システムの例が示されている。

【０００６】

【発明が解決しようとする課題】ところで、従来、インターネットは、パーソナルコンピュータ（以下、ＰＣ）やワークステーション（以下、ＷＳ）上で利用されてきたが、近年、ＰＣ以外の様々な機器においても利用が始まっている。例えばウェブの利用が可能な携帯情報端末や、携帯電話が登場してきている。

【０００７】これらの機器は小型で持ち運びが可能であり、携帯電話網のような無線網を経由してインターネットに接続することで、いつでもどこでも、インターネットを利用した電子商取引、バンキングサービスを利用することが可能になる。

【０００８】しかしながら、これらの機器は、一般にＰＣよりも処理速度が遅く、メモリ容量が小さく、搭載できるソフトウェアに対する制約が大きい。

【０００９】インターネットを利用した電子商取引、バンキングサービスに必要な、セキュリティ確保のための暗号化／復号化ソフトウェアやＳＳＬプロトコルは、複雑な計算を必要とし、ＰＣよりも処理能力が制限されている携帯情報端末で処理を行なうには負荷が大きく、サービスを円滑に提供できない可能性がある。

【００１０】ところで、携帯電話網を流れるデータは通常暗号化されており、携帯電話の端末には、元々そのデータの暗号化及び復号化機能が備わっている。

【００１１】即ち、携帯電話網はインターネットと異なり、通信網としてセキュリティが確保されている。

【００１２】そのため、セキュリティが確保されている通信網で利用される端末にとって、通信網が提供するセキュリティに加え、さらにインターネット上でのデータの送受信に必要な、暗号化及び復号化処理を行なうことは、余分な処理を行なっていると考えることができる。

【００１３】本発明は、かかる問題点に鑑みてなされたものであり、携帯電話網のような安全性が確保された通信網を経由してインターネットに接続し、電子商取引やバンキングサービスを実施する端末装置の負担を軽減することができる通信方法を提供し、また、その通信方法を実施する通信システムを提供することを目的としている。

【００１４】

【課題を解決するための手段】そこで、本発明の通信方法では、コンテンツデータを管理するコンテンツサーバ装置とコンテンツサーバ装置とは異なる通信網上に存在するクライアント装置とが、異なる通信網間を中継するゲートウェイサーバ装置を介して行なう通信において、クライアント装置及びゲートウェイサーバ装置間の通信の安全性が確保されている場合に、クライアント装置及びゲートウェイサーバ装置間の通信網ではデータの暗号化は行なわず、セキュリティが確保されていないゲートウェイサーバ装置及びコンテンツサーバ装置間の通信網による通信でのみデータの暗号化を行なうようにしている。

【００１５】また、この通信方法を実施する通信システムでは、クライアント装置に、ゲートウェイサーバ装置との間でデータの送受信を行なうデータ通信手段と、このデータ通信手段を通じてクライアント装置及びコンテンツサーバ装置間の通信の安全要求を送出する暗号化通信要求手段とを設け、ゲートウェイサーバ装置に、クライアント装置との間でデータの送受信を行なうクライアントデータ通信手段と、コンテンツサーバ装置との間でデータの送受信を行なうサーバデータ通信手段と、クライアント装置からの安全要求に従いサーバデータ通信手段を通じてコンテンツサーバ装置との暗号化通信の設定処理を行ない、サーバデータ通信手段から受信した暗号化されたデータの復号化とサーバデータ通信手段に出力するデータの暗号化とを行なう暗号化通信制御手段とを設けている。

【００１６】そのため、クライアント装置とコンテンツサーバ装置との間の全ての通信経路における安全性を確保しながら、クライアント装置への暗号化・復号化処理系の搭載を不要にし、クライアント装置の負担を軽減することができる。

【００１７】

【発明の実施の形態】本発明の請求項１に記載の発明は、コンテンツデータを管理するコンテンツサーバ装置とコンテンツサーバ装置とは異なる通信網上に存在するクライアント装置とが、異なる通信網間を中継するゲートウェイサーバ装置を介して行なう通信方法において、クライアント装置及びゲートウェイサーバ装置間の通信の安全性が確保されている場合に、クライアント装置及びゲートウェイサーバ装置間の通信網ではデータの暗号化は行なわず、セキュリティが確保されていないゲートウェイサーバ装置及びコンテンツサーバ装置間の通信網による通信でのみデータの暗号化を行なうようにしたものであり、クライアント装置には、暗号化通信の設定や、暗号化されたデータの復号化を行なう処理系を搭載する必要が無くなり、クライアント装置の負担が軽減される。

【００１８】請求項２に記載の発明は、クライアント装置が、ゲートウェイサーバ装置に対して、通信経路での安全要求を送出し、これを受けてゲートウェイサーバ装置がコンテンツサーバ装置との間で暗号化通信の設定を行ない、コンテンツサーバ装置が、クライアント装置に送信するデータを暗号化してゲートウェイサーバ装置に送信し、ゲートウェイサーバ装置が、データを復号化してクライアント装置に送信するようにしたものであり、コンテンツサーバ装置から送られるデータが、暗号化され安全に伝送される。

【００１９】請求項３に記載の発明は、クライアント装置が、ゲートウェイサーバ装置に対して、データの送信と併せて通信経路での安全要求を送出し、これを受けてゲートウェイサーバ装置がコンテンツサーバ装置との間で暗号化通信の設定を行ない、このデータを暗号化してコンテンツサーバ装置に送信するようにしたものであり、ゲートウェイサーバ装置からコンテンツサーバ装置に送られるデータを暗号化して安全に伝送することができる。

【００２０】請求項４に記載の発明は、コンテンツデータを管理するコンテンツサーバ装置とコンテンツサーバ装置とは異なる通信網上に存在するクライアント装置とが、異なる通信網間を中継するゲートウェイサーバ装置を介して通信を行なう通信システムにおいて、クライアント装置とゲートウェイサーバ装置との間が安全性が確

保された通信網で接続され、クライアント装置に、ゲートウェイサーバ装置との間でデータの送受信を行なうデータ通信手段と、このデータ通信手段を通じてクライアント装置及びコンテンツサーバ装置間の通信の安全要求を送出する暗号化通信要求手段とを設け、ゲートウェイサーバ装置に、クライアント装置との間でデータの送受信を行なうクライアントデータ通信手段と、コンテンツサーバ装置との間でデータの送受信を行なうサーバデータ通信手段と、クライアント装置からの安全要求に従いサーバデータ通信手段を通じてコンテンツサーバ装置との暗号化通信の設定処理を行ない、サーバデータ通信手段から受信した暗号化されたデータの復号化とサーバデータ通信手段に出力するデータの暗号化とを行なう暗号化通信制御手段とを設けたものであり、クライアント装置には、暗号化通信の設定や、暗号化されたデータの復号化を行なう処理系を搭載する必要が無くなり、クライアント装置の負担が軽減される。

【００２１】請求項５に記載の発明は、クライアント装置に、データ通信手段を通じてゲートウェイサーバ装置との間でワールド・ワイド・ウェブのデータを送受信するためのウェブプロトコル処理手段を設け、ゲートウェイサーバ装置に、クライアントデータ通信手段及びサーバデータ通信手段を通じてワールド・ワイド・ウェブのデータを送受信するためのウェブプロトコル処理手段を設けたものであり、ＨＴＴＰのようなウェブプロトコルを使用するデータ伝送の安全性を確保しながら、クライアント装置の負担を軽減することができる。

【００２２】以下、本発明の実施の形態について、図面を用いて説明する。

【００２３】この通信システムは、図１に示すように、携帯電話網400を通じて通信を行なうクライアント装置100と、異なる通信網である携帯電話網400とインターネット500とを中継するゲートウェイサーバ装置200と、インターネット500を通じてゲートウェイサーバ装置200に接続するコンテンツサーバ装置300とから成る。

【００２４】クライアント装置100は、クライアント装置100とコンテンツサーバ装置300との間でデータが安全に送受信されることを要求するリクエストを作成する暗号化通信リクエスト生成部101と、クライアント装置100とゲートウェイサーバ装置200とコンテンツサーバ装置300との間で共通に利用されるウェブの転送プロトコルＨＴＴＰ（Hyper Text Transfer Protocol）を処理するウェブプロトコル処理部102と、携帯電話網400との間でデータを送受信するデータ通信部103とを具備している。

【００２５】また、ゲートウェイサーバ装置200は、携帯電話網400との間でデータを送受信するクライアントデータ通信部201と、クライアント装置100、ゲートウェイサーバ装置200及びコンテンツサーバ装置300間で共通に利用されるウェブの転送プロトコルＨＴＴＰを処理するウェブプロトコル処理部202と、クライアント装置100からの要求を受けて、ゲートウェイサーバ装置200及びコンテンツサーバ装置300間での暗号化された安全な通信を確立し、データの暗号化及び復号化を行なう暗号化通信制御部203と、インターネット500との間でデータを送受信するサーバデータ通信部204とを具備している。

【００２６】また、コンテンツサーバ装置300は、インターネット500との間でデータを送受信するデータ通信部301と、ゲートウェイサーバ装置200からの要求を受けて、ゲートウェイサーバ装置200との間で暗号化された安全な通信を確立し、データの暗号化・復号化を行なう暗号化通信制御部302と、クライアント装置100、ゲートウェイサーバ装置200及びコンテンツサーバ装置300の間で共通に利用されるウェブの転送プロトコルＨＴＴＰを処理するウェブプロトコル処理部303とを具備している。

【００２７】この通信システムのクライアント装置100は、コンテンツサーバ装置300との安全な通信を希望する場合に、ゲートウェイサーバ装置200に対して、送信データの出力と併せて、ゲートウェイサーバ装置200及びコンテンツサーバ装置300間の暗号化通信を要求する。

【００２８】これを受けてゲートウェイサーバ装置200は、コンテンツサーバ装置300との間で暗号化通信の設定を行ない、送信データを暗号化してコンテンツサーバ装置300に送信する。コンテンツサーバ装置300も、また、クライアント装置100に送信するデータを暗号化してゲートウェイサーバ装置200に送信し、ゲートウェイサーバ装置200は、これを復号化してクライアント装置100に送信する図２は、この通信システムのクライアント装置100が、暗号化通信の確立要求を行なう場合の処理の流れを示している。

【００２９】ステップ601：暗号化通信リクエスト生成部101は、暗号化通信リクエストを作成し、
ステップ602：ウェブプロトコル処理部102は、暗号化通信リクエスト生成部101が生成した暗号化通信リクエストを基にウェブプロトコルにおけるウェブページ取得のリクエストを作成する。

【００３０】ステップ603：データ通信部103は、ウェブプロトコル処理部102が作成したウェブページ取得のリクエストを、携帯電話網400を通じゲートウェイサーバ装置200に送信する。

【００３１】図３は、この通信システムのゲートウェイサーバ装置200が、クライアント装置100から送信されたデータを受信した後の処理の流れを示している。

【００３２】ステップ701：クライアントデータ通信部201は、クライアント装置100から送信されたデータを受信するとウェブプロトコル処理部202に送り、
ステップ702：ウェブプロトコル処理部202は、クライアントデータ通信部201が受信したデータを解析して、
ステップ703：これがクライアント装置100からの暗号化

通信の確立要求を含むウェブリクエストであるか否かを判定する。暗号化通信の確立要求を含むウェブリクエストである場合には、暗号化通信制御部203を起動する。

【００３３】ステップ704：起動した暗号化通信制御部203は、コンテンツサーバ装置300に対して暗号化通信の設定要求をサーバデータ通信部204を通じて送信し、ステップ705：コンテンツサーバ装置300との間で暗号化通信を確立するための設定処理を行なう。

【００３４】ステップ706：次いで、暗号化通信制御部203は、ウェブプロトコル処理部202が解析したウェブページ取得リクエストを、この設定に従って暗号化し、サーバデータ通信部204に対して暗号化データを送信する。

【００３５】ステップ707：サーバデータ通信部204は、送信が依頼されたデータを、インターネット500を通じてコンテンツサーバ装置300に送信する。

【００３６】また、ステップ703において、解析したデータが暗号化通信の確立要求を含まない通常のウェブリクエストである場合には、ステップ707へ進み、サーバデータ通信部204に対してそのままウェブリクエストを送信する。

【００３７】コンテンツサーバ装置300では、データ通信部301がインターネット500から送られて来たデータを受信し、データが暗号化されている場合には、暗号化通信制御部302がこれを復号化し、ウェブプロトコル処理部303がウェブの転送処理を行なう。

【００３８】また、コンテンツサーバ装置300がクライアント装置100から要求されたデータを送信する場合には、ゲートウェイサーバ装置200との間で暗号化通信の設定処理が行なわれているときは、暗号化通信制御部302がデータを暗号化し、データ通信部301が暗号化されたデータをインターネット500に送出する。

【００３９】図４は、この通信システムのゲートウェイサーバ装置200が、コンテンツサーバ装置300から送信されたデータを受信した場合のその後の処理の流れを示している。

【００４０】ステップ801：サーバデータ通信部204は、コンテンツサーバ装置300からのデータを受信すると、ステップ802：このコンテンツサーバ装置300から受信したデータが暗号化されたデータか否かを判定し、暗号化されたデータである場合には、暗号化通信制御部203を起動する。

【００４１】ステップ803：暗号化通信制御部203は、サーバデータ通信部204で受信した暗号化データを復号化し、ウェブプロトコル処理部202に対して受信データを送信する。

【００４２】ステップ804：ウェブプロトコル処理部202は、受信したウェブレスポンスを解析し、クライアントデータ通信部201に対して解析したウェブレスポンスを送信する。

【００４３】ステップ805：クライアントデータ通信部201は、受信したウェブレスポンスを、携帯電話網400を通じてクライアント装置100に送信する。

【００４４】また、ステップ802において、コンテンツサーバ装置300から受信したデータが暗号化されたデータでない場合には、ウェブプロトコル処理部202に対して受信データを送信し、ステップ804、ステップ805の処理が行なわれる。

【００４５】図５は、クライアント装置100の暗号化通信リクエスト生成部101で生成される暗号化通信リクエストの例である。クライアント装置100は、図５中の「ｈｔｔｐｓ」というキーワードで、暗号化通信の確立を要求する。

【００４６】図６は、図５の暗号化通信リクエストから、クライアント装置100のウェブプロトコル処理部102が作成したウェブページ取得リクエストの例である。図６のウェブページ取得リクエストは、図５の暗号化通信リクエストを先頭とし、ウェブプロトコルとして必要な幾つかの情報を、ヘッダとして付け加えて構成されている。

【００４７】なお、暗号化通信確立のためのキーワードは、図５の例の「ｈｔｔｐｓ」に限定されるものではない。クライアント装置100、ゲートウェイサーバ装置200及びコンテンツサーバ装置300で使用するウェブプロトコル間において取り決められたキーワードであればよい。

【００４８】また、暗号化通信確立のためのキーワードは、図６の例のように、必ずしもウェブページ取得リクエストの先頭行になくともよい。例えば、ヘッダとしてリクエストの先頭以外に、暗号化通信確立の設定に必要な各種パラメータを記載することを可能にしてもよい。

【００４９】図７は、ゲートウェイサーバ装置200が図６のウェブページ取得リクエストをコンテンツサーバ装置300に送信したときに、コンテンツサーバ装置300からゲートウェイサーバ装置200に送信されてきた、暗号化されたデータを復号化した、ウェブレスポンスの例である。

【００５０】なお、本発明の実施の形態では、クライアント装置100とゲートウェイサーバ装置200との間のセキュリティが確保されている通信網を携帯電話網としているが、セキュリティの確保された通信網であればその他の通信網でもよく、本発明の適用は携帯電話網に限定されるものではない。

【００５１】また、本発明の実施の形態では、クライアント装置100、ゲートウェイサーバ装置200及びコンテンツサーバ装置300がウェブプロトコル（ＨＴＴＰ）を使用して通信しているが、本発明の適用はＨＴＴＰに限定されるものではない。

【００５２】

【発明の効果】以上の説明から明らかなように、本発明

の通信方法及び通信システムでは、セキュリティが確保されている通信網上のクライアント装置は、暗号化通信の要求をゲートウェイサーバに送信するだけで、コンテンツサーバ装置から送信されるデータを安全に受信することができる。そのため、クライアント装置に、暗号化通信の設定や、暗号化されたデータの復号化を行なう処理系を搭載する必要が無くなり、メモリの少ないＰＣ以外の機器であってもクライアント装置として用いることが可能になる。

【００５３】また、コンテンツサーバから受信するデータだけでなく、クライアント装置から送信するデータについても暗号化して安全に送信することができる。

【００５４】また、ＨＴＴＰのようなウェブプロトコルが使用される場合でも、セキュリティが確保されている通信網上のクライアント装置は、暗号化通信の設定や、暗号化されたウェブデータの復号化を行なう処理系を搭載しなくても、コンテンツサーバ装置との間で安全にデータを送受信することができる。

【図面の簡単な説明】

【図１】本発明の実施形態における通信システムの構成図、

【図２】実施形態の通信システムにおけるクライアント装置の動作を示すフローチャート、

【図３】実施形態の通信システムにおけるゲートウェイサーバ装置がクライアント装置からデータを受信したときの動作を示すフローチャート、

【図４】実施形態の通信システムにおけるゲートウェイサーバ装置がコンテンツサーバ装置からデータを受信したときの動作を示すフローチャート、

【図５】クライアント装置の暗号化通信リクエスト生成部で生成される暗号化通信リクエストの例、

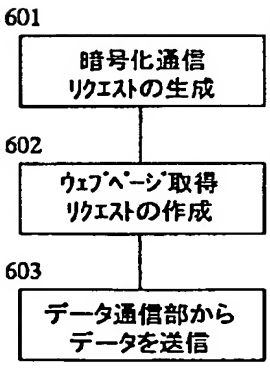
【図６】クライアント装置のウェブプロトコル処理部が作成したウェブページ取得リクエストの例、

【図７】ゲートウェイサーバ装置がコンテンツサーバ装置から受信したウェブレスポンスの例である。

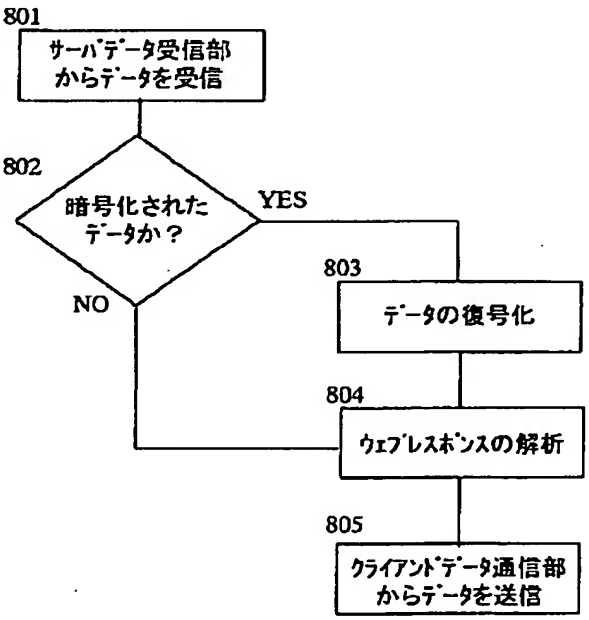
【符号の説明】

100　クライアント装置
101　暗号化通信リクエスト生成部
102　ウェブプロトコル処理部
103　データ通信部
200　ゲートウェイサーバ装置
201　クライアントデータ通信部
202　ウェブプロトコル処理部
203　暗号化通信制御部
204　サーバデータ通信部
300　コンテンツサーバ装置
301　データ通信部
302　暗号化通信制御部
303　ウェブプロトコル処理部
400　携帯電話網
500　インターネット

【図２】

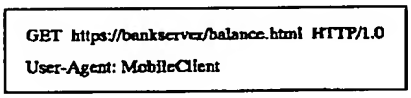


【図４】

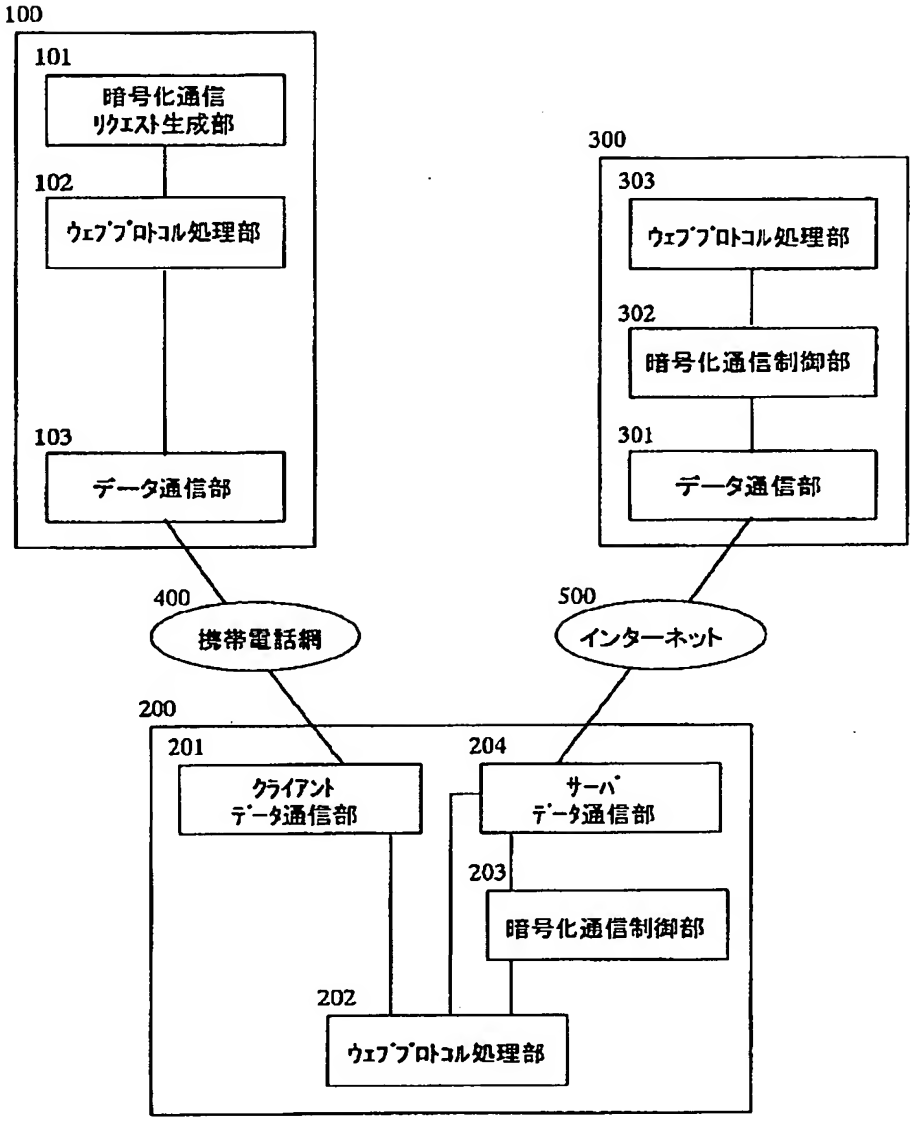


【図５】

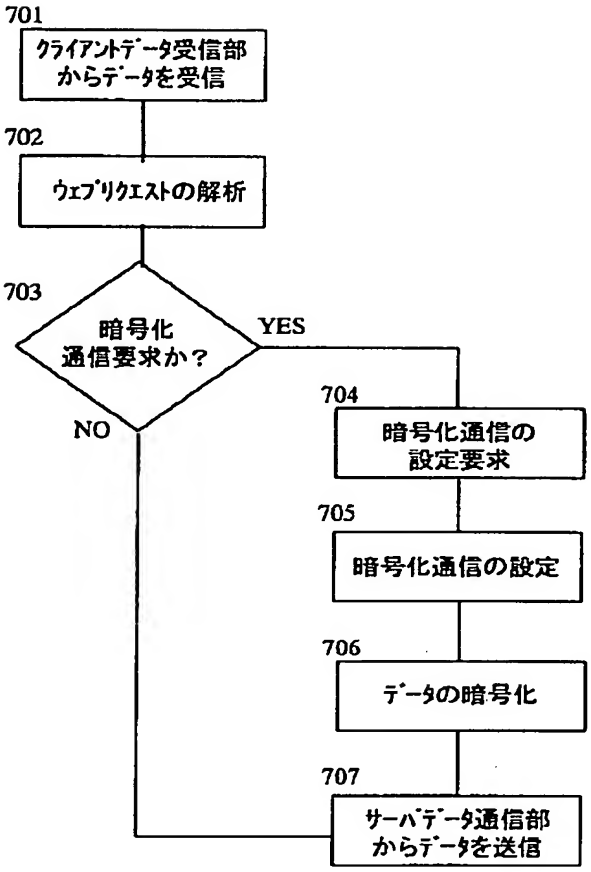
【図６】



【図１】


100
101
暗号化通信
ﾘｸｴｽﾄ生成部
102
ｳｪﾌﾞﾌﾟﾛﾄｺﾙ処理部
103
データ通信部
300
303
ｳｪﾌﾞﾌﾟﾛﾄｺﾙ処理部
302
暗号化通信制御部
301
データ通信部
400
携帯電話網
500
インターネット
200
201
ｸﾗｲｱﾝﾄ
ﾃﾞｰﾀ通信部
204
ｻｰﾊﾞ
ﾃﾞｰﾀ通信部
203
暗号化通信制御部
202
ｳｪﾌﾞﾌﾟﾛﾄｺﾙ処理部

【図３】



【図７】

```
HTTP/1.0 200 OK
Date: Mon,14 Dec 1998 13:00:00 GMT
Content-Length: 129
Content-Type: text/html

<HTML>
<BODY>
<CENTER>
<H1>残高照会</H1>
12月14日 13:00 現在の預金残高は
<BR>
￥128,000です。
</CENTER>
</BODY>
</HTML>
```

フロントページの続き

(72)発明者　浦　誠治
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　米本　佳史
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　和田　浩美
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　石垣　純二
神奈川県横浜市港北区網島東四丁目３番１号　松下通信工業株式会社内
(72)発明者　中土　昌治
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(72)発明者　佐々木　啓三郎
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内

Ｆターム(参考)　5J104 AA01 AA33 PA01 PA07 PA09 PA10
5K030 GA03 GA15 HC01 HC09 HD03 HD05 JT09
9A001 CC06 EE03 JJ25 JJ26 JJ27 KK56 LL03